

[NT] Microsoft ActiveSync Clear Text Password

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0030.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/08/05

To: list@securiteam.com

Date: 8 Aug 2005 13:16:33 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Microsoft ActiveSync Clear Text Password

SUMMARY

<<http://www.microsoft.com/windowsmobile/downloads/activesync37.msp>>

Microsoft ActiveSync is "widely used to synchronizes Windows based PDAs and smartphones with desktop computer. PDA can connect to PC via COM/USB/IR or LAN. Before synchronization user on PC must setup "partnership" to allow synchronization. If PDA is protected with password user on PC should provide password before he can access the device".

Synchronization over LAN/Wi-Fi has some design weakness, these include the password being sent in clear text.

DETAILS

Vulnerable Systems:

* ActiveSync version 3.8

1. All data, including initial "authentication", is transmitted in clear text. This has no security implication in the case of COM/USB and other physical protected communication, however, LAN (Wi-Fi in most cases) is very sensitive for sniffing, and such communication could be intercepted

2. Even if the PDA is password protected, ActiveSync doesn't ask password

Securiteam: [NT] Microsoft ActiveSync Clear Text Password

in case of network synchronization

3. ActiveSync doesn't use any form of authentication for server (PC) or client (PDA), therefore rogue server or fake clients can synchronize with the server/client without difficulty

You can discover ActiveSync that have the LAN synchronization by scanning for TCP port 5679:

```
nmap -p 5679 192.168.0.*
```

Fake server:

It is easy to build rogue server without any special software. All that is required is ActiveSync, a sniffer and any MitM condition.

Steps:

1. Install ActiveSync on rogue server. Enable network synchronization
2. Realize a MitM condition
3. Launch you favorite sniffer and set filter to save TCP packets on port 5679
4. Wait for PDA connection
5. Open sniffer and check second data packet from PDA. At offset 0x14 and 0x18 you can see partnerships ids. ActiveSync can support up to 2 PC and as you can see, PDA send both IDs in the "handshake"
6. Import template in registry. Change key
HKEY_CURRENT_USER\Software\Microsoft\Windows CE Services\Partners\<Partnership> to sniffed partnership id
7. Wait for another connection and check ActiveSync, device should be connected as "guest". Even if you got "Synchronization Error", try to click "Explore" button on the toolbar

Fake Client:

Is very similar to the rogue server, but you don't need MitM conditions to accomplish this attack. All that is need is the name of the PC and corresponding "partnership id"

1. Launch your favorite registry editor for Windows Mobile
2. Navigate to HKLM\Software\Microsoft\Windows CE Services\Partners\P1
3. Create string value PName = <PC_NAME>
4. Create DWORD value PId = <partnership id>
5. Launch active sync on PDA and try to connect. If everything is OK, synchronization will occur.

Mitigating factors:

1. LAN synchronization is disabled by default
2. To implement a "fake client" you would need to know that Partnership ID. It's hard to guess (2^{32}), but because ActiveSync accept 2 partnership ID per connection, actually we need (2^{31}) connections to brute force the string

ActiveSync should use TLS for authentication of PC and PDA and data encryption. We don't need PKI in this case, because "direct trust" can be

Securiteam: [NT] Microsoft ActiveSync Clear Text Password

created and certificates transmitted from PDA to PC and vice versa when "Partnership" is established

ADDITIONAL INFORMATION

The information has been provided by <mailto:Hataha_@_yandex.ru> Natalia Melnikova.

The original article can be found at:

<<http://www.securitylab.ru/56278.html>>

<http://www.securitylab.ru/56278.html>

The original article can be found at:

<<http://www.security.nnov.ru/Fnews64.html>>

<http://www.security.nnov.ru/Fnews64.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.